Is Sarnia-Lambton ready for the next cyber attack?

An outside look at the public-facing side of 1,270 small businesses that run their own website across Sarnia, Petrolia, Corunna, Forest, Grand Bend, Watford, and the county. No scanning, no business named.

36+

EXPOSED TO THE PHP TAKEOVER BUG

On an unpatched or unsupported PHP version. A floor, since most sites hide it. PHP2Shell is being exploited right now.

83%

CAN BE IMPERSONATED BY EMAIL

724 of 871 have no enforced DMARC.

82%

HTTPS SET UP PROPERLY

94 serve a broken or missing certificate.

The bug behind this report. PHP2Shell (CVE-2026-109618 and CVE-2026-109619) was disclosed October 21, 2026, rated 9.2 of 10, and lets an attacker take over a web server with no password. It is on the US CISA must-patch list. PHP runs most of the web, so it reaches ordinary small-business sites.

OP-01

WHERE THE GAPS ARE

Can be impersonated by email	724 · 83%
No SPF record at all	108 · 12%
On WordPress	388 · 40%
Behind on WordPress (of versions shown)	42 · 24%
Broken or missing HTTPS	94 · 10%

OP-02

ALSO FOUND

Businesses with their own website	1,270
Running WordPress	388
Taking card payments (WooCommerce)	111
Still loading a 2016 code library	52
Dead domains (no longer resolve)	232
Parked or placeholder pages	56

An abandoned domain can be re-registered by anyone, who then receives that business's email.

OP-03

5 FIXES THAT CLOSE MOST OF THE GAP

1. **Stop email spoofing.** Publish SPF, turn on DKIM, set DMARC to quarantine or reject.
2. **Patch the platform, hide the version.** Keep WordPress, plugins, and PHP current; turn off version numbers.
3. **Force HTTPS.** Redirect to the encrypted site and add an HSTS header.
4. **Turn on multi-factor authentication.** On the admin, the email, and the hosting panel. Remove old accounts.
5. **Mind unused domains.** Keep them renewed with mail off, or let them go on purpose.